The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	NO. CR16-5110 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	NO. CR15-387 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	NO. CR15-274 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**

I, Brian N. Levine, declare as follows:

1. I am a Professor of Information and Computer Sciences at the University of Massachusetts Amherst, where I have been a member of the tenure-track faculty since 1999. I am also the Director of the University of Massachusetts Amherst Cybersecurity Institute. I received my Ph.D. in Computer Engineering from the University of California Santa Cruz, where my dissertation focused on the Internet. My expertise includes the topics of digital forensics, Internet privacy and anonymity, network protocol design, network security, peer-to-peer networks and applications, and Internet-based child sexual exploitation crimes. I have been publishing in peer-reviewed scientific venues on these topics for twenty years. During that time, I have collaborated with industry, government, and academe on topics relevant to these cases, including Tor, network forensics, and child pornography investigations. My contributions range from designing new privacy enhancing technologies (e.g., for users of the Internet, cellular phones, and digital currencies) to quantifying the worldwide Internet-based trade of images of child sexual exploitation. I have designed and taught courses at the University of Massachusetts Amherst on Digital Forensics, Computer and Network Security, Advanced Information Assurance, Computer Networks, Data Structures, and Computer Crime Law. I have chaired major conferences and workshops in my field on digital forensics, mobile computing, and other topics. Since 2008, I have been working with agencies in the Department of Justice, including the Federal Bureau of Investigation, and with Internet Crimes Against Children Task Forces to build and deploy tools for forensic investigation of child pornography trafficking. None of those tools were a part of the above-referenced cases before this Court, and I was not involved in the investigation of the "Playpen" website. These experiences and others are detailed in my attached curriculum vitae. I am currently under contract with the FBI to provide research and development of tools and strategies for network-based investigation of Internet-based crimes against children, particularly on peer-to-peer file sharing networks. My work in reviewing the materials pertinent to this case and preparing this declaration is not being performed pursuant to

that contract. My work is being performed pursuant to a contract with the U.S. Attorney's Office for the Western District of Washington.

2. In preparing this declaration, I have reviewed the following: from *U.S. v. Michaud*, No. CR15-5351RJB, the declaration of Vlad Tsyrklevich dated January 13, 2016 (hereinafter "Tsyrklevich Dec."), the declaration of Robert Young dated May 2, 2016 (hereinafter "Young Dec."), the declaration of Shawn Kasal dated May 9, 2016 (hereinafter "Kasal Dec."), and the declaration of Dr. Matthew Miller dated May 9, 2016 (hereinafter "Miller Dec."); the declaration of Special Agent Daniel Alfin from *U.S. v. Matish*, No. 4:16cr16 filed June 1, 2016 (hereinafter "Alfin Dec."); the network packet capture (PCAP) evidence from the computers of Tippens, Lesan, and Lorente, and the corresponding FBI payload executables for each; excerpts of the Cygnus report for Tippens, Lesan, and Lorente that contain the FBI's recording of information collected by the NIT for each of their computers; the forensic examination reports for the devices of Lorente dated February 28, 2016, Lesan dated December 20, 2015, and Tippens dated July 11, 2016; the NIT warrant application (*In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion*, Case No. 1:15-SW-89 Eastern District of Virginia); and the complaint against Tippens dated February 11, 2016. I am advised that all of that information has been disclosed to or made available to the defendants for review.

3. I have not had access to nor did I review the source code or executable for the FBI exploit that deployed the NIT payloads. I also have not had access to nor did I review the FBI server or any "generator" code used to create unique identifiers.

4. Based on my review of available documents, my understanding of the overall process used by the FBI is as follows. A defendant's computer connected using the Tor network to the Playpen website, logging in with a specific username. Retrieving certain pages from the Playpen website resulted in the download of the FBI's *exploit* and *payload* programs. Much like a tool to open a locked door to a house, the purpose of the exploit was to allow for the execution of the payload program on a defendant's computer. The bespoke payload carried a *unique identifier* that was generated by the FBI, as well as

a *case identifier* common to all payloads generated for the Playpen operation. The payload program queried a defendant's computers for certain information, such as the hostname and operating system type. These details, along with the unique identifier and case identifier were sent by the payload program to an FBI server via the Internet. The action of sending data to the FBI over the Internet revealed the public IP address used by the defendants that was assigned by an Internet Service Provider (ISP) and linked to billing information. The exploit and payload did not persist on the defendants' computers after execution.

5. In this document, my references to "the exploit", "payload", "generator", "NIT", and "server" are reserved to the mechanisms employed by the FBI. My use of the term "malware" is reserved for computer programs that were created or deployed by third parties (i.e., neither the defendants nor the FBI) intending harm by, for example, downloading images of child sexual abuse to a computer unbeknownst to its owner.

6. From the materials available to me, I have concluded the following.

a. When viewed in the context of the facts of these cases, the declarations of Messrs. Tsyrklevich, Miller, Kasal, and Young contain many overbroad generalizations and implausible explanations, which are not rooted in cited or documented facts or evidence, and they are insufficient to support their hypotheses.

b. Specifically, *there is no evidence to support any of the following hypotheses* referenced in the defendants' submissions: the defendants did not visit the Playpen website; the information relayed by the payload to the FBI servers via the Internet was tampered with or altered by a third party; the identifiers generated by the FBI are not reliable; an FBI exploit or payload made permanent changes to the security settings or any other settings of the defendants' computers; an FBI exploit or payload are responsible for images of child sexual abuse found on the defendants' computers and in their residences.

c. A review of the exploit, software that generated unique identifiers, or server software is not necessary to show that these hypotheses are merely speculation premised upon extremely unlikely theoretical possibilities, as I detail below using only existing evidence.

(I) The evidence strongly supports the fact that the exploit and payload delivered from the Playpen website to the defendants' computers were transferred without modification or tampering.

7. *First*, none of the declarations contend or suggest that the defendants' computers did not visit the Playpen websites. The evidence strongly supports the fact that the defendants' computers did visit the site; the opposite conclusion would be explainable by only specific evidence of malware that has not been found and is not suggested to exist in any defense declaration.

8. *Second*, it stands without doubt that the exploit and payload were delivered with integrity because connections to Playpen were accepted only via tamperproof connections created and maintained by Tor. No declaration disputes this fact.

(II) The evidence strongly supports the fact that the exploit delivered from the Playpen website did not exceed the scope of the warrant.

9. We know from Special Agent Alfin's sworn statement that the exploit was restricted to allowing the payload to be delivered and executed and did not alter the settings of the computer (e.g., Alfin Dec. at 2 ¶ 6,8,9,14,17). I have reviewed no information in any of the defendants' submissions that shows otherwise. Let us consider, for the sake of argument, the possibilities listed in defense declarations for the exploit to instead "execute additional functions outside the scope of the NIT warrant" (Tsyrklevich Dec. at 3 ¶ 6)[1].

(II.a) Mr. Miller speculates that the exploit may have caused the defendants' computers to "crash, lose or alter data, and not respond to normal input" (Miller Dec. at 2 ¶ 4). First, while these outcomes are theoretically possible, I have reviewed no information in any of the defendants' submissions to explain how experiencing any of

[1] The Tsyrklevich declaration does not further expand on the possibilities.

those symptoms would result in any defendants' possession of images of child sexual abuse. I am aware of no plausible explanation for how perturbations of existing data can create child pornography. Second, this speculation is not supported by any information in the defendants' submissions that shows that any defendants' computers actually experienced any of those symptoms, demonstrated through forensic artifacts that link such events to an exploit.

(II.b) Mr. Miller's speculation about the exploit continues, "or it may alter any of the settings on that system. Depending on the exploit, it can affect the security posture of the computer going forward" (Miller Dec. at 2 ¶ 4) as well as "any devices that have been connected to it" (Miller Dec. at 2 ¶ 5). This statement is speculation that is not supported by any information in any of the defendants' submissions drawing from the defendants' computers. I would have expected that such statements would be based on evidence that resulted from an examination of the defendants' computers and devices demonstrating an affected "security posture" caused by the FBI's exploit or some third-party malware. Regardless, a changed setting, if ever found, is insufficient to explain evidence in these cases, as I discuss presently.

(II.c) Mr. Miller further states that "Without knowing what exploit was used by the FBI in this case, we cannot determine whether the files that the government says were located on various storage devices were put on those devices by Mr. Michaud." (Miller Dec. at 3 ¶ 7).

10. The conclusion that one "cannot determine" whether a defendant put images of child sexual abuse on his device without the exploit is wrong and misleading. Changed settings on a computer (if they occurred) alone cannot be singularly responsible for the presence of images of child sexual abuse. Some sort of third-party malware would have to have been responsible, under the defense's contention, for that to occur. In other words, *an examination of the exploit to determine how or if settings were changed, regardless of the outcome, would not shed light on whether some third-party actor delivered child pornography to a defendant's computer.* The defense would need to search

for evidence of malware, which they can do through an examination of the defendants' computers. Computers are always vulnerable to threats known and unknown, just as someone's home is always vulnerable to a break-in. Looking at a lock to determine whether it is broken, or can be picked, does not and cannot tell the homeowner what someone who might have broken or picked the lock did after entering the house. Similarly, reviewing one particular exploit would provide evidence that a defendant's computer was vulnerable to that one particular exploit, but it would shed no light upon the computer's potential vulnerabilities to innumerable others. Nor would it shed any light on what particular malware was or could have been delivered to that computer. Reaching that conclusion requires an examination of the computer.

11. Further, the defense submissions point to no evidence to suggest that the exploit or payload made fundamental changes or alterations to any defendants' computer system or disabled its firewall. Special Agent Alfin states under oath that "It is theoretically possible for *an* exploit to make fundamental changes or alterations to a computer system to disable its security firewall. However, as noted above, the NIT used here and the exploit used to deliver it did not do so", and he continues that "Other than to point to this theoretical possibility, I am aware of no evidence or indication to which either defense expert points to suggest otherwise." (Alfin Dec. at 3 ¶ 14). But even if we assume, for the sake of argument, that the exploit did modify a setting that could later have been exploited by third-party malware designed to download images of child sexual exploitation to the defendants' computers, reviewing the exploit would not shed any light on that malware for several reasons.

12. *First*, if such third-party malware did exist that could take advantage of an altered setting, it is significant that it has not, to my knowledge, been located by the defense team or the public. I would have expected the defendants' computers to be the first reasonable place to look for third-party malware. However, to my knowledge, either no such examination has taken place or the exam did not result in finding malware nor evidence of tampered settings, files, and systems.

13. *Second*, an assumption that the exploit changed settings would not refute the fact that the defendants' computers visited the Playpen website and requested data from it (so that the NIT would have been delivered), that the exploit and payload were delivered without tampering, or the accuracy of the information returned by the payload (a topic I return to below).

14. *Third*, certain evidence in each of these cases *cannot be explained as the result of a malware infection*:

a. The evidence report for Gerald Lesan states that "220 videos were identified," including footage of nude adults and minors in an identifiable location. "Additionally, there were videos that captured Gerald Lesan adjusting and slightly moving the camera…and exposing his penis toward the camera." No malware could have set up and personally adjusted this camera. There is no information in the defendants' submissions to indicate how malware could have been responsible for those actions, or how review of the exploit could possibly shed light on those actions.

b. The evidence report for Lorente states that "A blow up doll with a child's face attached and a hole in the mouth area, was seized at the search site and placed into evidence as item 1B1. SA Highley found an image file of this child's face on 1B23", where 1B23 refers to Lorente's Dell laptop computer. No malware could have downloaded an image of a child's face to Lorente's laptop, printed a hard copy, physically attached the print out to a blow up doll, and cut a hole in the mouth area. Again, defense offers no explanation of how malware or a review of the exploit could explain these facts.

c. The Tippens complaint states, "At the time of execution, Tippens was the only person in the home, and upon entering his bedroom, I saw that the large-screen television in that room was displaying a video depicting a young girl being sexually assaulted. Specifically, the video showed what appeared to be a young female, approximately three to five years old, being vaginally and anally penetrated by the hand of an adult male." Upon seeing such a video on a large screen, or upon hearing the sounds from such a video that must have quite obviously indicated the sexual abuse of a very young child, no malware could be responsible for allowing it to remain playing in one's own bedroom. Further, I have reviewed no information in any of the defendants' submissions that presents evidence (rather than unsupported speculation) of malware causing this video to be transferred to and played on the television without Tippens's knowledge.

(II.d) Mr. Kasal asks, "In this case, was the targeted computer vulnerable to receiving illegal content from the government's own child pornography site along with or after the initial NIT breach? Or more likely (because third party malware, viruses and remote attacks have advanced faster than law enforcement can keep up) did the government's NIT leave the target computer vulnerable to separate attacks and viruses?" (Kasal Dec. at 2 ¶ 6). In addition to the statements I've made above, the following points are relevant.

15. *First*, separate attacks and viruses are just that — separate — and to say that they cannot be found by an expert without access to the exploit is not a reasonable conclusion. Special Agent Alfin states the typical and more reasonable assumption of forensic analysis: "In each instance when I have been tasked with identifying and analyzing malware, I did not have advance knowledge of the specific malware for which I was looking or even if malware was actually present, though there was reason to suspect the presence of malware." (Alfin Dec. at 6 ¶ 30). The place to look for malware that has purportedly infected a computer is the computer itself.

16. *Second*, assume for the sake of argument that subsequent to the defendants' computers visiting the Playpen website and the exploit's execution, malware had command and control of their machines with the purpose of storing images of child sexual abuse. It is reasonable to expect that malware designed to furtively store images on the defendants' machines would also have the ability to later retrieve the images. To allow retrieval after a device reboot, such malware would need to reside in permanent storage, making it easier to find by experts, and yet it has not been found.

17. The defense has a team of experts with qualifications in "forensic analysis of computers and computer-based evidence…forensic software analysis and analysis of computer storage media and communications networks since 1988" (Young Dec. at 1 ¶ 1); "data forensics, and network threat attrition/attribution" (Kasal Dec. at 1 ¶ 2), and experience "in the collection and analysis of code necessary to audit the deployment of the NIT" in a "very similar" case (Kasal Dec. at 2 ¶ 3); training in "malware analysis" (Miller Dec. at 6), teaching of "Advanced Reverse Engineering" (Miller Dec. at 7), "prior work analyzing FBI 'Network Investigative Techniques'" (Miller Dec. at 1 ¶ 1); and "forensic analysis" (Tsyrklevich Dec. at 1 ¶ 1). They are clearly qualified to find evidence of malware, examples of settings that suggest malware, evidence of tampering, examples of data incongruities that begin to suggest tampering, etc. None have been found. All can be found without review of the exploit, but without such findings from the defendants' computers, specific supporting analysis, or other evidence, their declarations offer not more than speculation and general possibilities rather than sound conclusions.

18. **(II.e)** Mr. Kasal states regarding "remote attacks" (Kasal Dec. at 3 ¶ 6) that "Such attacks, often involving the transmission, storage and distribution of child pornography in particular, are well documented. The illicit child pornography industry and distribution networks are massive, and some of most sophisticated efforts to remote transmit and secretly store illegal content on the computers of unwitting Internet users (including corporations and large networks) have been developed by pornography distributors. I have even worked on a Nebraska state court case where the defendant's cell phone was infected with a virus that routed child pornography through and to that phone…It was not until exhaustive analysis was done that we discovered the extent of the infection." (Kasal Dec. at 3 ¶ 7). This statement is problematic for two primary reasons.

19. *First*, the story demonstrates that to support claims of malware, exhaustive analysis of infected *devices* is critical; notably, the defense has not reported similar success for these three defendants.

20. *Second*, it is unsound to conclude from a lone anecdote that malware is the

prevalent or common medium by which images of child sexual abuse is traded, distributed, or propagated. In contrast, in several peer-reviewed published articles[2], my research has documented the worldwide trafficking of images of child sexual abuse that is supported by popular, open, non-anonymous, peer-to-peer file sharing networks. In a recent publication[3] that reported on several years of measurements, we observed an average of over 800,000 unique computers per month sharing known images of child sexual abuse on file-sharing networks, such as BitTorrent. I am aware of no peer-reviewed, published articles documenting any "sophisticated efforts to remotely transmit and secretly store illegal content on the computers of unwitting Internet users" on the scale claimed by Mr. Kasal. (Kasal Dec. at 3 ¶ 7).

21. It also bears noting that my review of the packet capture traces, which recorded the information returned by defendants' computers, confirms that the payload operated to collect the particular information permitted by the authorizing warrant.

(III) The existing evidence strongly supports the fact that once the exploit and payload were delivered and executed, the information was returned accurately without an encrypted connection.

22. My examination of the packet capture (PCAP) traces shows that the payload's information was returned accurately to FBI servers. It is not an issue that these packets were not encrypted due to other protections that were in place, the realities of the Internet, and the facts of this case.

23. My review of the packet capture traces shows that each execution of the NIT payload resulted in either 9 or 10 packets. The traces represent a back-and-forth via a

[2] For example, see: (1) "Characterization of Contact Offenders and Child Exploitation Material Trafficking on Five Peer-to-Peer Networks," George Bissias, Brian Neil Levine, Marc Liberatore, Brian Lynn, Juston Moore, Hanna Wallach, and Janis Wolak. Elsevier Child Abuse & Neglect, 52:185–199, 2016. (2) "Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network," Janis Wolak, Marc Liberatore, and Brian Neil Levine. Elsevier Child Abuse & Neglect, 38(2):347–356, February 2014. (3) "Measurement and Analysis of Child Pornography Trafficking on P2P Networks," Ryan Hurley, Swagatika Prusty, Hamed Soroush, Robert J. Walls, Jeannie Albrecht, Emmanuel Cecchet, Brian Neil Levine, Marc Liberatore, Brian Lynn, and Janis Wolak. In Proc. Intl. World Wide Web Conference (WWW), May 2013. 11 pages.

[3] Bissias et al. 2016

connection initiated by the defendants' computers and accepted by the FBI server. Each packet contains the IP address of the computer that executed the NIT payload as source or destination. The exchanges occurred using the standard *Internet Protocol (IP),* which manages source and destination addressing and error detection for these values. The data within each packet is carried via the *Transmission Control Protocol (TCP)*, which includes reliability mechanisms that detect and recover from errors such as missing packets, corrupted data, and out-of-order delivery. The data itself conforms to the *Hypertext Transfer Protocol (HTTP)* and made to look as if a web page was requested from the FBI server. HTTP is used by browsers, such as Microsoft Internet Explorer and Google Chrome, to retrieve web pages. To draw an analogy, the IP protocol is similar to how the U.S. Postal Service expects and uses the *To:* and *From:* addresses written on an envelope; the TCP protocol is like sending a letter via certified mail with the addition that a copy is resent if the original is lost or damaged; and HTTP is like an order form requesting a specific item from a merchant.

24. The exchanges can be summarized as follows, ignoring small differences in the traces that result from varying network conditions.

a. A request for a reliable TCP connection is initiated by a defendant's computer to the FBI server.

b. The TCP connection is accepted by the FBI server, which in turn initiates a reliable TCP connection back to the defendant's computer.

c. The defendant's computer accepts the connection back.

d. Using the reliable TCP connection, the defendants' machines send, in a single packet, information if available (e.g., hostnames, operating systems, usernames, and MAC addresses), as well as the FBI's common operation identifier and the respective unique identifiers. These data appear in the standard format of a web page request.

e. The FBI server acknowledges to the defendant, using TCP, that the data indicating the web page request was received correctly (analogously, a postal return receipt), while also responding with a standard HTTP message that the requested web page is not available.

f. The defendant's computer and FBI server each signal that all data was received correctly and close the connection. This type of IP/TCP/HTTP exchange occurs many billions of times per day on the Internet. There is nothing out of the ordinary about the traces, including indications of third-party tampering or network-based attacks.

25. My comments focus on (1) unintentional errors and (2) intentional altering of information that could occur during these exchanges.

26. *First*, the traces strongly support the fact that the data was not unintentionally altered while in transit. Mr. Young asks if there was "an internal 'checksum' to ensure there are no errors in transmission?" for the unique identifier (Young Dec. at 4 ¶ 13). My review of the data confirms that *all packets in the packet capture trace contained two checksum fields* that ensure integrity during transmission. (Additional integrity checks are added in transit by "lower" network layers, such as Ethernet or Wi-Fi links, managed by Internet routers but would not be recorded in the trace.) The first checksum is part of every IP packet sent via the Internet and ensures the integrity of the packet *header*, which includes the IP addresses (analogous to the outside of a postal envelope). The second checksum is part of every packet's TCP segment, and it ensures the integrity of the *data* during transit (analogous to the contents of a postal letter). No examination of the exploit's source code is relevant to confirming the checksums. My inspection of the packets returned by the defendants' machines to the FBI server shows that both checksums in all packets were valid.

27. The failure rate of these two checksums makes errors near impossible for the packet containing the data returned by the payload in each trace. The checksums will always detect any error of less than 15 consecutive bits (i.e., roughly two characters in the packet). Longer consecutive bit errors have an extremely low rate of occurring but not being detected. Specifically, a highly cited peer-reviewed study of TCP checksums based on two-years of real Internet data found that "between one data packet every 16 million

packets and one packet in every 10 billion packets will have an undetected checksum error"[4] depending on several technical factors. These traces are 9–10 packets each with the payload results appearing in a single packet. This error rate or smaller applies to the IP header checksum, too. It is not only the same style and length checksum, but if the addresses had been corrupted, the packets could not have been routed back and forth successfully for the length of the traces; analogously, one cannot exchange letters back and forth via the postal service if the envelope has the wrong addresses.

28. *Second*, the facts of the case, the realities of the Internet, and logic strongly support the fact that the data was not intentionally altered or tampered with while in transit from the defendants' machines to the FBI servers. Several challenges prevent altering and tampering.

a. To intercept and tamper with the traffic returned by the payload would require privileged access to the routers controlled by Internet Service Providers (ISPs) carrying the packets *prior* to the time when the defendants' computers visited the Playpen website. Such interception would have to occur specifically at one of a set of routers limited to those between the FBI server and each of the defendants' computers[5]. In general, routers controlled by ISPs are protected by a professional information technology staff and it is reasonable to expect that was the case here.

b. An attacker in a position to alter traffic at a router would have to examine all traffic crossing the routers they controlled for packets destined to the FBI server. That implies they would have to have the ability to recognize packets associated with the FBI

[4] Jonathan Stone and Craig Partridge, "When the CRC and TCP Checksum Disagree." Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (ACM SIGCOMM) Pages 309–319. October 2000. Available from https://dl.acm.org/citation.cfm?id=347561"

[5] TCP is designed to protect against the tampering of unencrypted connections by third parties that are not in a position to observe the connection's packets. Specifically, TCP connections are considered as a sequence of bytes from sender to receiver. A counter appears in each packet and is incremented by the number of bytes sent. The initial value of the counter is not zero; instead it is a random value that is from a range that is too large to be successfully guessed blindly by an attacker that cannot observe the packets. Without knowing the value, packets cannot be inserted into the connection. The traces show that a large, non-zero value was selected in all three traces, allowing us to conclude that to be successful, a supposed attacker must have controlled a router along the path (or re-routed all Internet traffic for a defendant's machine to their own, which is just as unlikely).

payload program and rewrite packets in real time conforming to the FBI's unpublished format, which is extremely unlikely for this law enforcement sensitive operation.

c. This attack's advanced sophistication already makes it extremely unlikely. Further, *even if this were all true*, it would not explain why images of child sexual abuse were stored on the defendants' computers as that would require a distinct malware infection. The defense documents do not suggest or provide specific evidence of malware that can explain the presence of images of sexual abuse found on the defendants' computers and devices.

d. Even if all of the above held, including the presence of malware, it does not explain the camera manually positioned by Lesan himself, the photo of a child's face physically attached to a blow up doll found in Lorente's residence, or the video of the sexual abuse of a child under 5 years old transferred to and left playing on Tippens's large-screen television.

29. In short, an attacker would have needed to have voluminous, non-public information about the FBI's investigation and each of the defendants' computers, access to Internet routers[6] protected by ISPs, along with sophisticated malware to gain access to and then place images of sexual abuse on the defendants' machines and place physical evidence in their residences, to even be capable of conducting such an attack. I have reviewed no information suggesting that to be the case.

(IV) The existing evidence strongly supports the fact that the data was stored and reproduced with integrity.

30. Mr. Tsyrklevich overstates the challenge involved when he states that the

[6] We need not consider an attacker that tampers with packets from within the defendants' local network, such as Wi-Fi broadcast from an Access Point (AP). Modifications made by the attacker to the IP address in the packet header would be overwritten by the AP before forwarding to the ISP's router on its way to the FBI server (or dropped by the AP). The same attacker could not have altered the unique identifier in the packet's TCP data since they could not have successfully guessed a valid identifier generated by the FBI server before the NIT was deployed. Specifically, the chances of successfully guessing a unique identifier selected by the FBI is less than 1 in 10^{33}. Notably, this scenario has no relevance to the exploit. Further, defense documents provide no evidence or facts that suggest such a scenario occurred in these cases.

FBI's "server component that stores the identifying information returned by the payload must faithfully store and reproduce the data it was sent. The correct use of data storage primitives and the programming practices used to avoid data corruption or tampering make analyzing this component of the NIT essential to understanding the digital 'chain of custody' of information derived from the NIT." (Tsyrklevich Dec. at 3 ¶ 6).

31. This statement overstates the challenge because access to the server component is not required to confirm data integrity. The checksums (detailed above) in the packets returned to the FBI server that are recorded in the packet traces confirm that the data's integrity was not disturbed. The packet captures associated with each defendant also show that the data recovered by the NIT from each defendant's computer matches what was sent to the FBI. That the same information exists in the FBI server logs is only a further redundancy rather than a necessary confirmation.

(V) The existing evidence strongly supports the fact that the identifiers were reliably unique.

32. Mr. Young states, "Another key consideration is the reliability of the 'identifier' used on [sic] connection with seized data." (Young Dec. at 3 ¶ 11). This concern stems from the purpose of the unique identifier, which is to allow the FBI to link activity of a user on the Playpen site to the IP address returning packets from a deployed NIT payload. The identifiers are also an administrative convenience for the FBI to know that all payload results were initiated by only an FBI-generated exploit.

33. Mr. Young continues, that the information provided to him "does not include, for example, such basic information as whether the FBI used a 'unique number generator' program to create their ID numbers. If so, what algorithm and what 'probability of collision' (chance of a duplicate) does that algorithm have? Did they just start at 1 and add 1 until they had a number that hadn't already been used?" (Young Dec. at 4 ¶ 13). Relatedly, Mr. Tsyrklevich states, "It is important to note that the errors in the use of cryptographic identifiers hinges on the correct use of a 'Pseudo-Random Number Generator,' a fundamental cryptographic technology that is frequently misused. Without

the missing data, I am unable to make a determination about these issue." (Tsyrklevich Dec. at 3 ¶ 6).

34. These concerns are easily answered without access to the source of the identifiers: the "generator" source code and executable and FBI server. Regardless of how the unique values were generated, all questions above can be addressed by evaluating the list of unique values themselves. Special Agent Alfin's sworn statement says that, "I have reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated." (Alfin Dec. at 5 ¶ 6). Checking for duplicates is trivial — an identifier would literally appear twice, no code review is required — and so I find it impossible to raise doubts about Special Agent Alfin's sworn answer. Regardless of speculation about the theoretical probabilities of collision, Special Agent Alfin's examination of the output shows that the *actual error* is zero.

35. The statements in the defense declarations grossly overstate the difficulty of picking a unique identifier. The purpose of the unique identifier in the NIT payload was *not* to seed a cryptographic operation, but merely to distinguish payloads as they were returned. It is a role that is closer to the tracking numbers assigned to packages shipped by Federal Express or the U.S. Postal service. The problem of duplicates itself is overstated by the defense declarations because the packet traces are timestamped, and the payloads need only be distinguished during the window of time from their deployment to their return. In the three trace files I examined, the entire exchange between the defendants' computers and the FBI server was completed in under 1 second, which is an extremely small window for error even if identifiers were repeated during the FBI's operation.

36. Additional assurances about the integrity of identifiers can be found from examining the information in the packet traces. In each of the three cases, the unique identifiers are 128-bits long, and so the total number of possible identifiers is 2^{128}, that is, a value larger than 10 followed by 37 zeros. To put it another way, if the FBI had

randomly generated unique identifiers for 20 trillion visitors to the Playpen website during the two-week operational window, the chances that any two pairs of identifiers would be duplicates is less than 1 in 1,000,000,000,000. Since the number of visitors must have been many, many fewer, the probability of one or more duplicates is much, much lower. Again, in any case, the actual error was observed to be zero. (Alfin Dec. at 5 ¶ 6). Notably, an attacker attempting to guess an identifier selected by the FBI will have an even lower chance of success.

37. As stated above, as the identifiers were transported through the Internet via TCP packets, checksums in the TCP header ensured that the values were not subject to unintentional error. And the advanced sophistication required of an attacker determined to re-write the data precludes intentional tampering.

38. Mr. Tsyrklevich's comparison to a cryptographic process is misleading. The FBI's process is more accurately described as a simplified version of a commonplace process deployed by Google on Android smartphones worldwide. Notably, Google's Android smartphone operating system accounts for over 85% of all smartphones[7], having sold over 1 billion mobile devices worldwide[8]. Generally, when an Android phone user clicks a website's advertisement for an "app" (i.e., software) and subsequently downloads, installs, and launches the app from the "Google Play" store, it is common that Google will send the app a unique value contained in the clicked advertisement[9]; the app is designed to take the value and send it to an analytics platform (e.g., operated by Google or the advertising company), revealing the user's IP and other information. Similarly, when a user clicked a link on a page on the Playpen website and subsequently

[7] "Global mobile OS market share in sales to end users from 1st quarter 2009 to 1st quarter 2016" Statista. http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/ (retrieved September 20, 2016)

[8] "Gartner Says Tablet Sales Continue to Be Slow in 2015", Gartner. January 5, 2015. http://www.gartner.com/newsroom/id/2954317 (retrieved September 20, 2016).

[9] See Google's developer documentation, including https://developers.google.com/android/reference/com/google/android/gms/tagmanager/InstallReferrerReceiver (retrieved September 20, 2016) or https://developers.google.com/analytics/devguides/collection/android/v4/campaigns (retrieved September 20, 2016).

downloaded the FBI payload, it contained a unique value; the payload was designed to take the value and send it to the FBI servers, revealing the user's IP and other information. This process is one that is relatively simple and easily repeatable and is not prone to the sort of rate of error or misuse that the defendants' submissions suggest.

EXECUTED: September 22, 2016.

BRIAN N. LEVINE, Ph.D.

Brian Neil Levine

140 Governors Drive
Amherst, MA 01060

Professional Experience

- **University of Massachusetts, Amherst, MA**
  Professor, College of Information and Computer Sciences — Sept. 2010–present
  Director, UMass Cybersecurity Institute

  Associate Professor, Department of Computer Science — Sept. 2005–August 2010
  Assistant Professor, Department of Computer Science — Sept. 1999–August 2005
  Research interests focus on security and networking; including topics within peer-to-peer networking and applications, forensics, privacy, mobile systems, and disruption-tolerant networks.

- **Fiksu, Inc.**, Boston, MA — June 2012–June 2013
  Vice President, Research: Real-time bidding networks; empirical analysis, optimization, and algorithmic design in the context of "big data" (~13k events per second) production system.
- **Intel Research**, Cambridge, UK — July 2004
  Visiting Researcher. Topics: disruption-tolerant networking.
- **Sprint Advanced Technology Laboratories**, Burlingame, CA — July–Aug. 2000
  Consultant. Topics: mirror servers on the Internet.
- **Sprint Advanced Technology Laboratories**, Burlingame, CA — July–Aug. 1999
  Consultant. Topics: deployment of multicast on the Internet.
- **University of California — Santa Cruz**, Santa Cruz, CA — Oct. 1994–June 1999
  Research Assistant. Topics: multicast-related protocols.
- **Institut National de Recherche en Informatique et en Automatique (INRIA)**, Sophia-Antipolis, France — May–Aug. 1998
  Research Intern. RODEO project. Topics: large-scale multicast applications.
- **Lucent Technologies, Bell Laboratories**, Holmdel, NJ — June–Sept. 1997
  Research Intern. Networking Software Research Department. Topics: IP multicast.
- **Sun Microsystems Laboratories**, Mountain View, CA — June–Sept. 1996
  Research Intern. High-Speed Networking group. Topics: ATM-based reliable multicast.

Education

- **Ph.D. in Computer Engineering**, June 1999
  University of California — Santa Cruz
  Dissertation: "Network Support for Group Communication", Advisor: Prof. J.J. Garcia-Luna-Aceves
- **M.S. in Computer Engineering**, June 1996
  University of California — Santa Cruz
  Master's Thesis: "A Comparison of Known Classes of Reliable Multicast Protocols",
  Advisor: Prof. J.J. Garcia-Luna-Aceves
- **B.S. in Applied Mathematics & Computer Science**, May 1994
  State University of New York at Albany
  Phi Beta Kappa, *magna cum laude,* Dean's List every semester, Cumulative GPA 3.73/4.00.
  New York State Regent's Scholarship (1990)

Fellowships and Awards

- *UMass Spotlight Scholar* (May 2016). Scholars are faculty who have demonstrated academic quality and leadership, nominated from tenure-track and non-tenure-track faculty on the Amherst campus.
- *Runner-up for Best Paper Award* at the 2013 International World Wide Web (WWW) Conference for "Measurement and Analysis of Child Pornography Trafficking on P2P Networks" (Hurley et al.); Out of 122 accepted papers (and 831 submissions).
- Co-advised Aruna Balasubramanian's dissertation, which received the *Runner-up ACM SIGCOMM Doctoral Dissertation Runner-up award* in 2011. (Co-advisor: Arun Venkataramani)
- *2011 Outstanding Research Award,* College of Natural Sciences, UMass Amherst. Awarded in part for work in digital forensics and crimes against children. Presented each year to two faculty from across 16 departments.
- *2008 Alumni Award for Excellence in Science & Technology* from the University at Albany (SUNY).
- *2007 Outstanding Teacher Award*, College of Natural Sciences & Mathematics, UMass Amherst. Awarded in part for working with undergraduates in research, curriculum and course development, and classroom activities.
- *Outstanding Paper award* at *ISOC Symposium on Network and Distributed System Security (NDSS) 2004* for "An Analysis of the Degradation of Anonymous Protocols" (Wright, Adler, Levine, and Shields).
- *Lilly Teaching Fellow*. Run by the UMass Center for Teaching (CFT). This competitive program is based on applicant's student teaching evaluations and a project proposal. The yearlong program includes collaboration with the CFT on individual projects and discussions with other Fellows to share ideas and experiences related to teaching excellence at the college level.
- Recipient of a National Science Foundation (NSF) *Faculty Early Career Development (CAREER)* award. This $410,000 grant is a prestigious NSF award for new faculty members.

Keynotes

1. Keynote, "Thwarting Internet-based Sexual Exploitation Crimes Against Children", Yahoo Tech Pulse conference, Sunnyvale, CA, December 2015
2. Keynote, "Fighting Internet-based Sexual Exploitation Crimes Against Children", Sixth International Systems and Storage Conference (SYSTOR), held in cooperation with USENIX and the Technion Center of Excellence (TCE). Haifa, Israel, June 2013.
3. Keynote, "Deployment of a Diverse, Outdoor Mobile Testbed," ICST Workshop on Networking in Public Transportation. Waterloo, Canada, August 2006.

Publications

Statistics

According to Google (http://scholar.google.com/citations?user=oHbIF48AAAAJ) as of August 2016:

- 14,500 citations total
- h-index of 47; and 36 papers with at least 100 citations each.

Peer-Reviewed Journal Articles

1. George D. Bissias, Brian N. Levine, Marc K. Liberatore, Brian Lynn, Juston Moore, Hanna Wallach, and Janis Wolak, "Characterization of Contact Offenders and Child Exploitation Material Trafficking on Five Peer-to-Peer Networks." *Elsevier Child Abuse & Neglect*, 52:185–199, 2016
2. George Bissias, Brian Levine, Marc Liberatore, and Swagatika Prusty, "Forensic Identification of Anonymous Sources in OneSwarm." *IEEE Transactions on Dependable and Secure Computing*, to appear 2016. 14 pages
3. Marc Liberatore, Brian Levine, Clay Shields, and Brian Lynn, "Efficient Tagging of Remote Peers During Child Pornography Investigations." *IEEE Transactions on Dependable and Secure Computing*, 11(5):425–439, September 2014.
4. Janis Wolak, Marc Liberatore, and Brian Levine, "Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network". *Child Abuse & Neglect*, 38(2):347–56. February 2014.

5. N. Boris Margolin, Brian Levine, James D. Miller, and Matthew Wright, “Economic incentives for protecting digital rights online.” *Electronic Commerce Research and Applications*. 10(5):553–564, September 2011.
6. Marc Liberatore, Bikas Gurung, Brian Levine, and Matthew Wright, “Empirical Tests of Anonymous Voice Over IP.” *Elsevier Journal of Computer Networks and Applications.* Journal of Network and Computer Applications. January 2011. 34(1):341–350.
7. Aruna Balasubramanian, Brian Levine, and Arun Venkataramani, “DTN Routing as a Resource Allocation Problem”. *IEEE/ACM Transactions on Networking (TON)*. April 2010. 18(2):596–609.
8. Nilanjan Banerjee, Mark D. Corner, and Brian Levine, “An Energy-Efficient Architecture for DTN Throwboxes.” *IEEE/ACM Transactions on Networking (TON)*. April 2010. 18(2):554–567.
9. Brendan Burns, Oliver Brock, and Brian Levine, “MORA Routing and Capacity Building in Disruption-Tolerant Networks”. *Elsevier Ad hoc Networks Journal*. 2008. 6(4):600–620. June 2008.
10. Matthew Wright, Micah Adler, Brian Levine, and Clay Shields. “Passive-Logging Attacks Against Anonymous Communications Systems”. *ACM Transactions on Information and System Security (TISSEC)*, 2008. 11(2). 34 pages. May 2008.
11. Jim Partan, Jim Kurose, and Brian Levine. “A Survey of Practical Issues in Underwater Networks “, *Special Issue of ACM Mobile Computing Communications Review* (selected papers from WUWNet 2007 that were further reviewed), 11(4):23–33. October 2007.
12. Nathaniel E. Baughman, Marc Liberatore, and Brian Levine, “Cheat-Proof Playout for Centralized and Distributed Online Games”. *IEEE/ACM Transactions on Networking (ToN).* 15(1):1–13. February 2007.
13. Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Levine, Clay Shields, and Elizabeth Belding-Royer, “Authenticated Routing for Ad hoc Networks”. *IEEE/ACM Journal of Selected Areas in Communications. (JSAC) Special Issue on Wireless Ad hoc Networks.* 23(3):598–610. March 2005. (Acceptance rate: 31/159, 20%).
14. Jeffrey Arnold, Brian Levine, R. Manmatha, Francis Lee, Prashant Shenoy, M.-C. Tsai, T.K. Ibrahim, D. O’Brien, D.A. Walsh, “Information Sharing in Out-of-Hospital Disaster Response: The Future Role of Information Technology”. *Journal of Prehospital and Disaster Medicine*. 19(3):201–207. July–September 2004.
15. Matthew Wright, Micah Adler, Brian Levine, and Clay Shields, “Analysis of the Degradation of Anonymous Protocols”. *ACM Transactions on Information and Systems Security* (TISSEC). 7(4):489–522. November 2004. (Submitted *by invitation.*)
16. Brian Levine and Clay Shields, “Hordes: A Protocol for Anonymous Communication Over the Internet”. *ACM Journal of Computer Security (JCS)*. 10(3):213–240. September 2002. (Submitted *by invitation.*)
17. Brian Levine, Sanjoy Paul, and J.J. Garcia-Luna-Aceves, “Organizing Multicast Receivers Deterministically According to Packet-Loss Correlation”. *ACM Multimedia Systems Journal*. 9(1):201–210. October 2002.
18. Christophe Diot, Brian Levine, Brian Lyles, H. Kassan, and Doug Balsiefien, “Deployment Issues for the IP Multicast Service and Architecture”. *IEEE Network, Special Issue on Multicasting*. 14(1):78–88. January 2000. Editor: Sanjoy Paul. (n.b., *IEEE Network* is a highly reviewed magazine; Acceptance rate: 6/60, 10%)
19. Brian Levine and J.J. Garcia-Luna-Aceves, “A Comparison of Reliable Multicast Protocols”. *ACM Multimedia Systems Journal*, 6(5):334–348. August 1998.

Peer-Reviewed Conference Papers, Workshop Papers, and Extended Abstracts

20. Robert J. Walls, Yuriy Brun, Marc Liberatore, and Brian Neil Levine, “Discovering Specification Violations in Networked Software Systems.” In Proc. IEEE International Symposium on Software Reliability Engineering (ISSRE), November 2015. (Acceptance Rate: 55/172; 32%)
21. George Bissias, A. Pinar Ozisik, Brian Levine, and Marc Liberatore. “Sybil-Resistant Mixing for Bitcoin.” In Proc. ACM Workshop on Privacy in the Electronic Society, November 2014. 10 pages. (Acceptance Rate: 17/67; 25%)
22. Saksham Varma, Robert J. Walls, Brian Lynn, and Brian Levine, “Efficient Smart Phone Forensics Based on Relevance Feedback.” In Proc. ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 12 pages. November 2014. (Acceptance Rate: 11/29; 38%)
23. Keen Sung, Brian Levine, and Marc Liberatore, “Location privacy without carrier cooperation.” In Proc. IEEE Workshop on Mobile System Technologies (MoST), 10 pages. May 2014. (Acceptance rate: 11/30; 37%).
24. Hamed Soroush, Keen Sung, Erik Learned-Miller, Brian Levine, and Marc Liberatore. “Turning off GPS is Not Enough: Cellular location leaks over the Internet.” In Proc. Privacy Enhancing Technologies Symposium (PETS), pp. 103–122, July 2013. (Acceptance rate: 13/69; 19%)
25. Ryan Hurley, Swagatika Prusty, Hamed Soroush, Robert J. Walls, Jeannie Albrecht, Emmanuel Cecchet, Brian Levine, Marc Liberatore, Brian Lynn, and Janis Wolak, “Measurement and Analysis of Child Pornography Trafficking on P2P

Networks." *Runner-Up, Best Paper Award.* In Proc. Intl. World Wide Web Conference (WWW), 11 pages, May 2013. (Acceptance rate: 122/831; 15%)

26. Sookhyun Yang, Jim Kurose, and Brian Levine, "Disambiguation of Residential Wired and Wireless Access in a Forensic Setting." In Proc. IEEE INFOCOM Mini-Conference, April 2013. 5 pages. (Acceptance rate: 129/1613 in mini-conference, with 274/1613 in main conference; 25%)
27. Robert J. Walls, Shane S. Clark, and Brian Levine. "Functional Privacy or Why Cookies are Better with Milk." In Proc. USENIX Workshop on Hot Topics in Security, August 2012. 6 pages. (Acceptance rate: 11/39; 28%)
28. James W. Partan, Jim Kurose, Brian Levine, and James Preisig. "Low Spreading Loss in Underwater Acoustic Networks Reduces RTS/CTS Effectiveness." In Proc. ACM International Workshop on UnderWater Networks (WUWNet), December 2011. 8 pages. (Acceptance rate: 19/24; 79%)
29. H. Soroush, P. Gilbert, N. Banerjee, B. N. Levine, M. Corner, and L. Cox. "Concurrent Wi-Fi for Mobile Users: Analysis and Measurements." In Proc. ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT), 12 pages, December 2011. (Acceptance rate: 30/159; 19%)
30. Hamed Soroush, Nilanjan Banerjee, Mark Corner, Brian Levine, and Brian Lynn. "A retrospective look at the UMass DOME mobile testbed" ACM SigMobile Mobile Computing and Communications Review (MC2R), 15(4):2–15, October 2011. (Invited paper)
31. Swagatika Prusty, Brian Levine, and Marc Liberatore. "Forensic Investigation of the OneSwarm Anonymous Filesharing System." In Proc. ACM Conference on Computer & Communications Security (CCS), 13 pages, October 2011. (Acceptance Rate: 60/429; 14%)
32. Robert J. Walls, Brian Levine, Marc Liberatore, and Clay Shields. "Effective Digital Forensics Research is Investigator-Centric." In Proc. USENIX Workshop on Hot Topics in Security (HotSec), August 2011. 7 pages. (Acceptance rate: 11/56; 20%).
33. Robert J. Walls, Erik Learned-Miller, and Brian Levine. "Forensic Triage for Mobile Phones with DEC0DE." USENIX Security, August 2011. 14 pages. (Acceptance rate: 35/204; 17%)
34. George Bissias, Brian Levine, and Ramesh Sitaraman. "Assessing the Vulnerability of Replicated Network Services." In *Proc. ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, 12 pages, November 2010. (Acceptance rate: 28/147; 19%)
35. Marc Liberatore, Brian Levine, and Clay Shields. "Strengthening Forensic Investigations of Child Pornography on P2P Networks." In *Proc. ACM Conference on Future Networking Technologies (CoNEXT),* 12 pages, November 2010. (Acceptance rate: 28/147; 19%)
36. John Tuttle, Robert J. Walls, Erik Learned-Miller, and Brian Levine, "Reverse Engineering for Mobile Systems Forensics with Ares." In *Proc. ACM Workshop on Insider Threats,* 8 pages, October 2010. (Acceptance rate: 7/12; 58%)
37. Marc Liberatore, Robert Erdely, Thomas Kerle, Brian Levine, and Clay Shields. "Forensic Investigation of Peer-to-Peer File Sharing Networks." In *Proc. DFRWS Annual Digital Forensics Research Conference*, 11 pages August 2010. (Acceptance rate: 16/39; 41%)
38. Brian Levine and Marc Liberatore, "DEX: Digital Evidence Exchange for Reproducibility, Comparison, and Reliability." In *Proc. of DFRWS Annual Conference on Digital Forensics,* August 2009. 9 pages. (Acceptance rate: 15/40; 38%)
39. Hamed Soroush, Nilanjan Banerjee, Aruna Balasubramanian, Mark D. Corner, Brian Levine, and Brian Lynn, "DOME: A Diverse Outdoor Mobile Testbed." In *Proc. ACM Intl. Workshop on Hot Topics of Planet-Scale Mobility Measurements (HotPlanet)*, 6 pages. June 2009. (Acceptance rate: 5/13; 38%)
40. Brian Levine and Gerome Miklau, "Auditing and Forensic Analysis." In M. Tamer A-Zsu and Ling Liu, editors, *Encyclopedia of Database Systems*. Springer-Verlag, June 2009. 6 pages.
41. Aruna Balasubramanian, Brian Levine, and Arun Venkataramani, "Enabling Interactive Web Applications in Hybrid Networks." In *Proc. ACM MobiCom*, pp. 70–80. September 2008. (Acceptance rate: 31/264; 12%)
42. Nilanjan Banerjee, Mark D. Corner, Don Towsley, and Brian Levine. "Relays, Base Stations, and Meshes: Enhancing Mobile Networks with Infrastructure." In *Proc. of ACM MobiCom*, pp. 81–91. September 2008. (Acceptance rate: 31/264; 12%)
43. Aruna Balasubramanian, Ratul Mahajan, Arun Venkataramani, Brian Levine, John Zahorjan, "Interactive WiFi Connectivity for Moving Vehicles." In *Proc. ACM SIGCOMM,* pp. 427–438. August 2008. (Acceptance rate: 36/288; 13%)
44. N. Boris Margolin and Brian Levine "Quantifying Resistance to the Sybil Attack." In *Proc. Financial Cryptography and Data Security (FC)*, pp. 1–15. January 2008. (Acceptance rate: 26/89; 30%)
45. John Burgess, George Bissias, Mark D. Corner, and Brian Levine, "Surviving Attacks on Disruption-Tolerant Networks without Authentication." In *Proc. of The ACM International Symposium on Mobile Ad hoc Networking and Computing (MobiHoc)*, pp. 61–70. September 2007. (Acceptance rate: 27/146; 19%)

46. Xiaolan Zhang, Jim Kurose, Brian Levine, Don Towsley, and Honggang Zhang, "Study of a Bus-Based Disruption Tolerant Network: Mobility Modeling and Impact on Routing." In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MobiCom),* pp. 195–206. September 2007. (Acceptance rate: 26/233; 11%)
47. Aruna Balasubramanian, Yun Zhou, W. Bruce Croft, Brian Levine, and Arun Venkataramani, "Web Search on a Bus." In *Proc. ACM Workshop on Challenged Networks (CHANTS),* pp. 59–66. September 2007. (Acceptance rate: 11/29; 38%)
48. Aruna Balasubramanian, Brian Levine, and Arun Venkataramani, "DTN Routing as a Resource Allocation Problem". In *Proc. ACM SIGCOMM*, pp. 373–384. August 2007. (Acceptance rate: 35/258; 14%)
49. Patrick Stahlberg, Gerome Miklau, and Brian Levine, "Threats to Privacy in the Forensic Analysis of Database Systems". In *Proc. ACM Intl Conf. on Management of Data (SIGMOD)*, pp. 91–102. June 2007. (Acceptance rate: 69/480; 14%)
50. George Bissias, Brian Levine, "Bounding Damage From Link Destruction with Application to the Internet." in *Proc. ACM SIGMETRICS,* pp. 367–368. June 2007. (Acceptance rate: 48/170, 28%; i.e., 170 submissions, of which 29 were accepted as full papers, 17 were accepted as extended abstracts.)
51. Nilanjan Banerjee, Mark D. Corner, and Brian Levine, "An Energy-Efficient Architecture for DTN Throwboxes." In *Proc. IEEE Infocom*, pp. 776–784. May 2007. (Acceptance rate: 252/1400; 18%)
52. N. Boris Margolin and Brian Levine, "Informant: Detecting Sybils Using Incentives." In *Proc. Financial Cryptography (FC),* pp. 192–207. February 2007 (Acceptance rate: 17/100; 17%).
53. Gerome Miklau, Patrick Stahlberg, and Brian Levine, "Securing History: Privacy and Accountability in Database Systems". In *Proc. Biennial ACM/VLDB Conference on Innovative Data Systems Research (CIDR),* pp. 387–396. Jan 2007 (Acceptance rate: 35/80; 44%)
54. Marc Liberatore, Brian Levine, Chadi Barakat, "Maximizing Transfer Opportunities in Bluetooth DTNs." In *Proc. ACM Conference on Future Networking Technologies (CoNext),* 11 pages. December 2006. (Acceptance rate: 19/86; 22%)
55. Marc Liberatore and Brian Levine. "Inferring the Source of Encrypted HTTP Connections." In *Proc. ACM conference on Computer and Communications Security (CCS),* pp. 255–263. October 2006. (Acceptance rate: 38/256; 15%)
56. Wenrui Zhao, Yang Chen, Mostafa Ammar, Mark D. Corner, Brian Levine, and Ellen Zegura. "Capacity Enhancement using Throwboxes in DTNs". In *Proc. IEEE Intl Conf on Mobile Ad hoc and Sensor Systems (MASS),* pp. 31–40. October 2006. (Acceptance rate: 49/197; 25%)
57. Jim Partan, Jim Kurose, and Brian Levine. "A Survey of Practical Issues in Underwater Networks." In *Proc. ACM International Workshop on UnderWater Networks (WUWNet),* pp. 17–24. September 2006. (Acceptance rate: 10/30; 33%)
58. Brendan Burns, Oliver Brock, Brian Levine, "Autonomous Enhancement of Disruption Tolerant Networks", In *Proc. IEEE International Conference on Robotics and Automation (ICRA),* pp. 2105–2110. May 2006 (Acceptance rate 39%)
59. Chris Piro, Clay Shields, and Brian Levine , "Detecting the Sybil Attack in Ad hoc Networks". In *Proc. IEEE/ACM International Conference on Security and Privacy in Communication Networks (SecureComm),* pp. 1–11. August 2006. (Acceptance rate: 32/126; 25%)
60. John Burgess, Brian Gallagher, David Jensen, Brian Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks". *Proc. IEEE INFOCOM*, 11 pages. May 2006 (Acceptance rate: 252/1400; 18%)
61. Matt Yurkewych, Brian Levine, and Arnold Rosenberg, "On the Cost-Ineffectiveness of Redundancy in Commercial P2P Computing." In Proc. *ACM conference on Computers & Communications Security (CCS),* pp. 280–288. November 2005. (Acceptance rate: 38/249; 15%)
62. Andrew Fast, David Jensen, Brian Levine, "Creating Social Networks to Improve Peer-to-Peer Networking." In *Proc. ACM Intl. Conf. on Knowledge Discovery and Data Mining (KDD),* pp. 568–573. August 2005 (Short Paper) (acceptance rate: 76/465, 16%. Specifically, 465 papers submitted to KDD; of those 40 were accepted as full papers and 36 were accepted as short papers, with the remainder rejected.)
63. Aaron St. John and Brian Levine, "Supporting P2P Gaming When Players Have Heterogeneous Resources." In Proc. *ACM Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV),* pp. 1–6. June 2005. (Acceptance rate: 33/88; 38%)
64. George Bissias, Marc Liberatore, David Jensen, and Brian Levine, "Privacy Vulnerabilities in Encrypted HTTP Streams." In *Proc. Privacy Enhancing Technologies Workshop (PET),* pp. 1–11. May 2005. (Acceptance rate: 18/71, 25%)
65. Brendan Burns, Oliver Brock, Brian Levine, "*MV* Routing and Capacity Building in Disruption Tolerant Networks." In *Proc. IEEE INFOCOM*, pp. 398–408. March 2005. (Acceptance rate: 244/1419, 17%)
66. N. Boris Margolin, Matthew K. Wright, Brian Levine, "Analysis of an Incentives-based Protection System." In *Proc. ACM Digital Rights Management Workshop (DRM),* pp. 22–30. October 2004. (Acceptance rate: 10/37, 27%)
67. Haizheng Zhang, Bruce Croft, Victor Lesser, Brian Levine, "A Multi-agent Approach for Peer-to-Peer based

Information Retrieval System." In *Proc. Intl. Joint Conference on Autonomous Agents and Multi Agent Systems (ICAPS)*, pp 456–464. June 2004. (Acceptance rate: 142/592, 24%)

68. Jacky Chu, Kevin Labonte, Brian Levine, "An Evaluation of Chord using Traces of Peer-to-Peer File Sharing", (extended abstract) in *Proc. ACM SIGMETRICS/Performance,* pp. 432–433. June 2004. (Acceptance rate: 22/252, 17%; i.e., 252 submissions, 21 full papers, 22 extended abstracts)
69. N. Boris Margolin, Matthew K. Wright, Brian Levine, "SPIES: Secrets Protection Incentives-based Escrow System." In *Proc. Second Workshop on the Economics of Peer-to-Peer Systems* (P2PEcon), 6 pages. June 2004. (Acceptance rate: 23/63, 37%)
70. Brian Levine, Mike Reiter, Chenxi Wang, and Matthew Wright, "Timing Attacks in Low-Latency Mix Systems." In *Proc. Financial Cryptography (FC),* pp 251–265 February 2004. (Acceptance rate: 17/78, 22%)
71. Katrina M. Hanna, Brian Levine, and R. Manmatha, "Mobile Distributed Information Retrieval for Highly Partitioned Networks." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP),* pp. 38–47. November 2003. (Acceptance rate: 30/230, 13%)
72. Matthew Wright, Micah Adler, Brian Levine, and Clay Shields, "Defending Anonymous Communication Against Passive Logging Attacks." In *Proc. IEEE Symposium on Security and Privacy*, pp. 28–41. June 2003. (Acceptance rate: 19/131, 15%)
73. Daniel Bernstein, Zhengzhu Feng, Brian Levine, and Shlomo Zilberstein, "Adaptive Peer Selection." In *Proc. Intl. Workshop on Peer-to-Peer Systems (IPTPS)*, pp. 237–246. February 2003. (Acceptance rate: 27/165, 16%)
74. Kimaya Sanzgiri, Bridget Dahill, Brian Levine, Clay Shields, and Elizabeth Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP),* pp. 78–89. November 2002. (Acceptance rate: 32/217, 15%)
75. Jacky Chu, Kevin Labonte, and Brian Levine, "Availability and Locality Measurements of Peer-to-Peer File Systems." In *Proc. ITCom: Scalability and Traffic Control in IP Networks II Conferences*, 12 pages. SPIE Vol. #4868. July 2002. (By invitation.)
76. Matthew Wright, Micah Adler, Brian Levine, and Clay Shields, "An Analysis of the Degradation of Anonymous Protocols." In *Proc. ISOC Network and Distributed System Security Symposium (NDSS)*, pp. 38–50. February 2002. *Received the Outstanding Paper Award.* (Acceptance rate: 16/79, 20%)
77. James Davis, Andy Fagg, and Brian Levine, "Wearable Computers as Packet Transport Mechanisms in Highly Partitioned Ad hoc Networks." In *Proc. IEEE Intl. Symposium on Wearable Computers (ISWC),* pp. 141–148. October 2001. (Acceptance rate: 36/157, 23%)
78. Vincent Scarlata, Brian Levine, and Clay Shields, "Responder Anonymity and Anonymous Peer-to-Peer File Sharing." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP)*, pp. 272–280. November 2001. (Acceptance rate: 36/157, 23%)
79. Katrina M. Hanna, Nandini Natarajan, and Brian Levine, "Evaluation of a Novel Two-Step Server Selection Metric." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP),* pp. 290–300. November 2001. (Acceptance rate: 36/157, 23%)
80. Nathaniel E. Baughman and Brian Levine, "Cheat-Proof Playout for Centralized and Distributed Online Games." In *Proc. IEEE INFOCOM*, pp. 104–113. April 2001. (Acceptance rate: 192/830, 23%)
81. Clay Shields and Brian Levine, "A Protocol for Anonymous Communication Over the Internet." In *Proc. ACM Conference on Computer and Communication Security (CCS),* pp. 33–43. November 2000. (Acceptance rate: 28/131, 21%)
82. Joerg Walz and Brian Levine, "A Hierarchical Multicast Monitoring Scheme." In *Proc. Intl. Workshop on Networked Group Communication (NGC),* pp. 105–116. November 2000. (Acceptance rate: 12/49, 25%)
83. Brian Levine, Jon Crowcroft, Christophe Diot, J.J. Garcia-Luna Aceves, and James F. Kurose, "Consideration of Receiver Interest for IP Multicast Delivery." In *Proc. IEEE INFOCOM*, pp. 470–479. March 2000. (Acceptance rate: 192/735, 26%)
84. Brian Levine, Sanjoy Paul, and J.J. Garcia-Luna-Aceves, "Organizing Multicast Receivers Deterministically According to Packet-Loss Correlation." In *Proc. ACM Intl. Multimedia Conference (Multimedia),* pp. 201–210. September 1998. (Acceptance rate unpublished)
85. Brian Levine and J.J. Garcia-Luna-Aceves, "Improving Internet Multicast with Routing Labels." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP),* pp. 241–250. October 1997. (Acceptance rate: 32/81, 40%)
86. Brian Levine, David Lavo, and J.J. Garcia-Luna-Aceves, "The Case for Concurrent Reliable Multicasting Using Shared Ack Trees." In *Proc. ACM Intl. Multimedia Conference (Multimedia)*, pp. 365–376. November 1996. (Acceptance rate: 40/142, 28%)
87. Brian Levine and J.J. Garcia-Luna-Aceves, "A Comparison of Known Classes of Reliable Multicast Protocols." In *Proc. IEEE Intl. Conference on Network Protocols (ICNP),* pp. 112–121. October 1996. (Acceptance rate: 31/96, 32%)

Selected Professional Service

- Founder, Steering Committee member (Sept 2015–present), Co-Organizer Sept 2015 and May 2016, *New England Security Day*
- Editorial Board member/Associate Editor: *IEEE Transactions on Mobile Computing* (Feb 2015–present)
- Editorial Board member/Associate Editor: *Journal of Privacy Enhancing Technologies* (September 2014–March 2016)
- Technical Program Chair. *Annual DFRWS Digital Forensics Research Conference* 2012
- Technical Program Co-Chair. *ACM MobiCom* 2011
- Technical Program Vice Chair. *Annual DFRWS Digital Forensics Research Conference*
- Associate Editor. *IEEE/ACM Transactions on Networking.* From September 2005–December 2010
- Guest Co-Editor. *IEEE Journal on Selected Areas in Communications (JSAC) special issue: Network Support for Multicast Communications*. October 2002, 20(8).
- Guest Co-Editor. *Computer Communications (Elsevier), Special Issue: Network Security*. 2006.
- Co-founder, co-organizer ACM First Annual Northeast Digital Forensics Exchange Workshop (NeFX) 2009, 2010
- Technical Program Co-chair and Co-organizer. ACM International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2006)
- Technical Program Co-Chair and Co-Organizer. Intl. Workshop on Networked Group Communication (NGC 2002)
- Recent Technical Program Committee service (as a member): ACM conference on Computer and Communication Security (CCS) 2006, 2008, 2009, 2013; Digital Forensics Research Conference (DFRWS) 2009–2013, 2015; ISOC Network & Distributed System Security Symposium (NDSS) 2012, 2014; Privacy Enhancing Technologies Symposium (PETS): 2003, 2004, 2005,2006, 2014; Annual Computer Security Applications Conference (ACSAC) 2014, 2015, 2016; Research on Attacks, Intrusions and Defenses (RAID) 2015

Experience as a Technical Expert

- For Shaevel & Krems, LLP (Boston, MA). As an expert witness "in computer engineering and security and privacy relative to it, and computer networking" for an arbitration case (American Arbitration Association). June 2005.

In public service settings:

- Invited public testimony to the US Sentencing Commission hearing on "Federal Child Pornography Offenses" in Washington, DC on February 15, 2012. Chaired by Honorable Patti B. Saris (United States District Court Judge), and convened with five other commissioners present.
- Member of the Internet Safety Technical Task Force Technical Advisory Board created by joint agreement of the Attorneys General Multi-State Working Group on Social Networking and MySpace.com. June–Oct. 2008. (See http://cyber.law harvard.edu/research/isttf/TAB)
- Member of the *Privacy Working Group* of the Secretary of Public Safety and Security, Massachusetts (Chairman: Secretary Kevin Burke), September 2008–2010.

Service to Dept. of Computer Science, UMass Amherst

- **Director, UMass Cybersecurity Institute,** September 2015–present. Coordinating engagement of faculty with industry partners and government, the creation of new educational programs and degrees, and hiring of new faculty in security, from the College of Information and Computer Sciences across to many other departments and colleges at UMass.
- **Undergraduate Program Director**, **Honors Program Director,** September 2009–June 2012. Led the department's growth from a 250-student department to enrollments exceeding 500 students, while deploying a newly designed BS degree and newly created BA degree.
- **Principal**, Center for Academic Excellence in Information Assurance Education & Research (CAEIAE-R). One of many Centers accredited through an application to the U.S. National Security Agency. From 2003–2015, when we elected to leave the program.

Selected Research Funding

Statistics**:** Over $11 million in funding as lead PI total, with additional funding as co-PI. Selected awards/contracts below.

1. PI: B. Levine, Co-PIs: W. Burleson, M. Liberatore, M. Sherman, E. Sommers, "CyberCorps Scholarship for Service at the University of Massachusetts Amherst," National Science Foundation. January 2016. (DGE-1565521)
2. PI: B. Levine, Co-PI: E. Learned-Miller, Office of Naval Research, "Triage-based Analysis of Mobile Phones". August 2012. (NPS-N00244-12-1-0057)

3. PI: B. Levine, Co-PI: M. Liberatore, "Strengthening Forensic Science for Network Investigations", Aug 2010. with partner UNH Crimes Against Children Research Center. National Science Foundation. (CNS-1018615).
4. PI: B. Levine, Co-PI: D. Goeckel "Novel Forensic Analysis for Crimes Involving Mobile Systems" National Science Foundation. September 2009 (CNS-0905349).
5. PI: B. Levine, Co-PI: M. Corner, "Slivers and Slices in a Diverse, Outdoor, Mobile Network Testbed" National Science Foundation GENI program. August 2008. (Project number 1599; NSF Award CNS-0714770)
6. PI: B. Levine, Co-PI: M. Corner, "NeTS-NBD: Construction of Robust and Efficient Disruption Tolerant Networks". National Science Foundation. (CNS-0519881). August 2005.
7. PI: B. Levine, Co-PIs: G. Miklau, "Collaborative Research: A Northeast Partnership for Developing the Information Assurance Workforce"; National Science Foundation. August 2008 (DUE-0830876)
8. PI: M. Corner Co-PI: B. Levine, "DOME: DTN Outdoor Mobile Environment" third phase of contract DARPA W15P7T-05-C-P213. August 2008
9. PI: M. Corner Co-PI: B. Levine, "DOME: DTN Outdoor Mobile Environment" second phase of contract DARPA W15P7T-05-C-P213. August 2006.
10. PI: B. Levine Co-PIs: M. Corner "ALERT: Adaptive LEarning and Routing Technologies for Disruption Tolerant Networks". Defense Advanced Research Projects Agency (DARPA) BAA04-13. October 2004. Contract W15P7T-05-C-P213.
11. PI: B. Levine, NSF CAREER grant, "Advances in Peer-to-Peer Networking". National Science Foundation. May 2002. NSF-0133055.
12. PI: B. Levine, NSF CISE Special Projects, "Collaborative Research: Anonymous Protocols". National Science Foundation. September 2001. NSF-0087482.

Teaching Experience

University of Massachusetts, Amherst, MA
Courses I have created and taught:

- CS 591SP *Digital Currencies* (Spring 2017, Spring 2016) (originally entitled *Multidisciplinary Security & Priva*cy)
- CS 391L *Computer Crime Law* (Fall 2015, Fall 2014; Fall 2011 with co-instructor; and as CS391LI/691LI: *Legal Issues in Computing* in Fall 2010)
- CS 365: *Digital Forensics* (Spring 2015; Spring 2010, Fall 2010, Fall 2008, Fall 2007) and CS491cc: *Advanced Digital Forensics* (Spring 2008)
- CS660: *Advanced Information Assurance* (Spring 2005; Fall 2006 with co-instructor)
- CS491Q/691Q: *System Building for Mobile Devices* (Spring 2003 with co-instructor; Spring 2004, Fall 2004)
- CS460: *Introduction to Computer and Network Security* (Spring 2001, Spring 2002, Spring 2003, Spring 2004, and Fall 2004 with co-instructor)
- CS653 *Advanced Computer Networks* (Fall 2000 and Fall 2001)

Other courses I have taught:

- CS187: *Data Structures* (Spring 2012)
- CS453: *Computer Networks* (Spring 2000, Fall 2009)
- Co-instructor, CE252 *Computer Networks* (graduate), Jan. 1999. (At UC Santa Cruz)
- Co-instructor, CE152 *Computer Networks* (undergraduate), Oct. 1998. (At UC Santa Cruz)